Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims

1. (Cancelled)

2. (Previously Presented) The method according to claim 10 wherein said open key is transmitted by adding it to a header of the transmission.

3. (Previously Presented) The method according to claim 9 wherein said base key is encrypted using a public key encryption algorithm.

4. (Currently Amended) The method according to claim 9 wherein said packet data is encrypted using a symmetric encryption algorithm in conjunction with said packet keys.

5. (Currently Amended) The method according to claim 11 wherein the secure hash is based on a hash function selected from the a group comprising SHA-1 and MD5.

6. (Cancelled)

7. (Cancelled)

8. (Cancelled)

9. (Currently Amended) A method for securely transmitting streaming media, the method comprising:

generating a random base key;

encrypting the streaming media by creating [[a]] <u>different</u> packet key<u>s</u> for each data

packet of the streaming media and encrypting each data packet using the corresponding packet keys, the packet keys being based on the base key and unique packet tags assigned to each data packet;

encrypting the base key, thus creating an open key; and

transmitting the encrypted data packets, ~~the packet key,~~ the ~~base~~ open key, and the unique packet tags to a recipient.

10. (Cancelled)

11. (Currently Amended) The method of claim 9 wherein the packet keys [[is]] are based on a secure hash of the base key and unique packet tags assigned to each data packet.

12. (Previously Presented) The method according to claim 3 wherein said public key encryption algorithm is asymmetric.

13. (Currently Amended) A method of receiving encrypted streaming media, the method comprising:

receiving an encrypted packet stream and an encrypted base key, the packet stream comprising a plurality of packets, each packet comprising encrypted packet information and a unique tag value;

extracting the unique tag value from each packet;

decrypting the encrypted base key;

computing a unique packet key for each packet based on the unique tag value and the ~~encrypted base~~ decrypted base key; and

decrypting the packet information using the corresponding packet keys.

14. (Previously Presented) The method according to claim 13 wherein said base key is encrypted using a public key encryption algorithm.

15. (Currently Amended) The method of claim 13 wherein the computation of the packet keys is based on a secure hash of the base key and the unique packet tags assigned to each data packet.

16. (Currently Amended) The method according to claim 15 wherein the secure hash is based on a hash function selected from ~~the~~ a group comprising SHA-1 and MD5.